QSC 18 | QUALYS SECURITY CONFERENCE 2018

Qualys Agents and RTI's

Leveraging Vulnerability Intelligence and Cloud Agents in Vulnerability Management: Prioritizing Risk at Montana State University

Constantine Vorobetz
Technical Account Manager, U.S. West, Qualys, Inc.

Agenda

Vulnerability Intelligence

Situation

Problems

Objectives

Technology

Results

Q&A

Qualys.

Vulnerability Intelligence

How it Works and How its Used

Intelligence vs. Information

Intelligence is information that has been analyzed

Intelligence provides informative insights

Collecting, processing, analyzing informatior

Data meets some goal or purpose

The problem is not to find something … But to understand something

Source: Multiple

Vulnerability Intelligence

Identifies the Vulnerabilities with the greatest impact on risk.

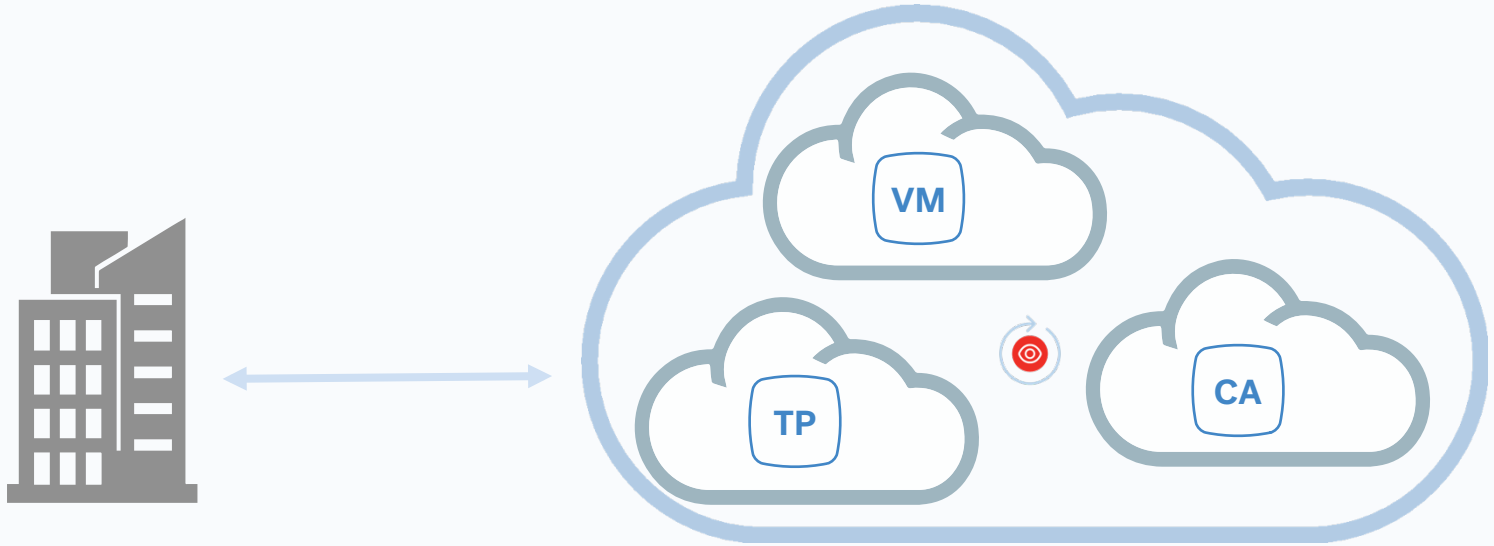
Proactive vs reactive.

Pertains to a specific environment.

Prioritizes vulnerability workflow.

Qualys.

We need to think about…

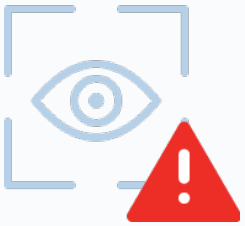


Threats and Vulnerabilities

Visibility with Technology

Situation Vulnerabilities/ Remediation

Information Overload



1. 19,299 vulnerabilities on 698 servers (2015)
2. Average Resolution 44.2 days
3. High numbers
4. Overwhelmed Staff
5. VM became a low priority
6. Can we be more proactive?

Objectives

Discover and Prioritize by Criticality

Effective Vulnerability Management Assesses the Risk

Verified and Reliable Data

Timely and Actionable

Technology

Cloud Agent & Threat Protect

Qualys Cloud Agent

Produces real-time data that is more reliable than traditional scanning.

More visibility into systems for troubleshooting, services running, user accounts, open ports, software and version number

Cloud Agent

Continuous Visibility and Real-Time Vulnerability Management:

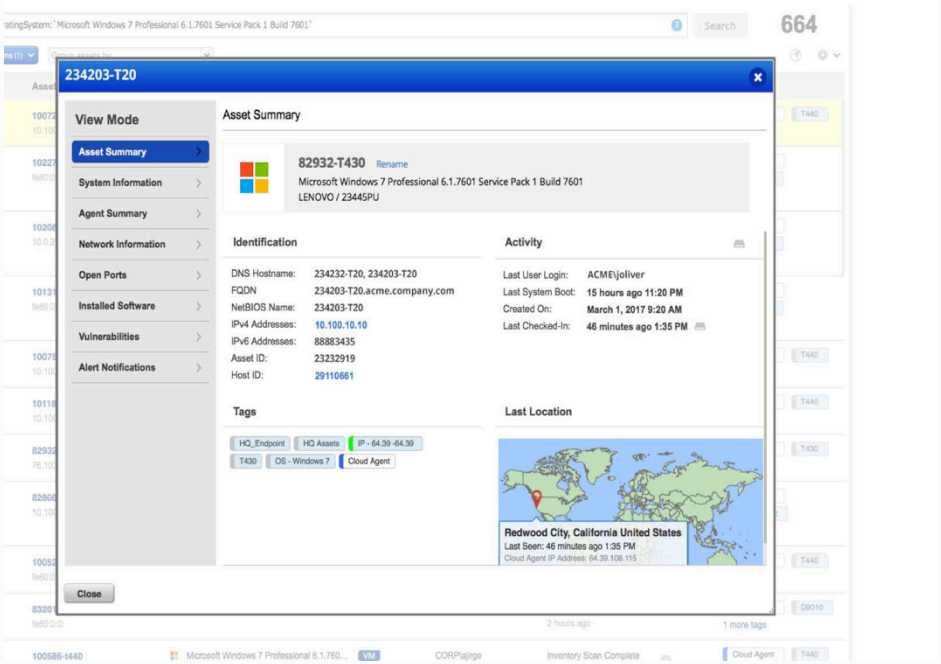
Continuous Data Collection

Eliminates scanning windows

Real-time tracking

No credentials to manage

Visibility of Operating System, Applications and Certificate.



Qualys.

Qualys Threat Protect

Real-Time Indicators (RTI's) are data points collected per vulnerability.

It is accurate, timely and actionable information to help prioritize and shrink the flood of Vulnerabilities reported

Threat Protect

Qualys.

Identify & Weigh Characteristics that Intensify a Vulnerabilities Danger:

Vulnerabilities that are not very critical can be dealt with in due course.

Know the assets with the most risk.

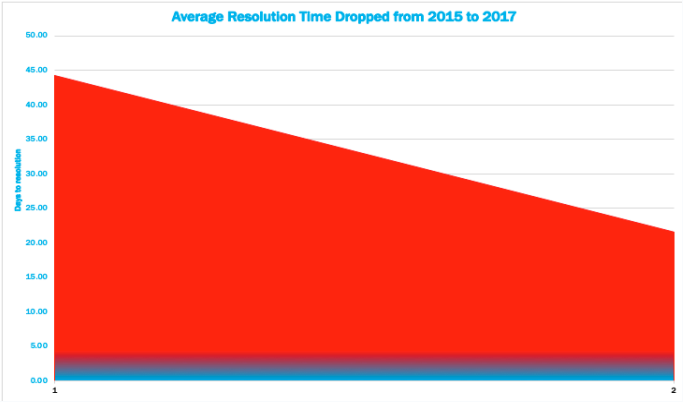
Prioritize based on criticality.

Understand the associations across vulnerabilities to know the impact of a threat.

Qualys.

Results Vulnerabilities/ Remediation

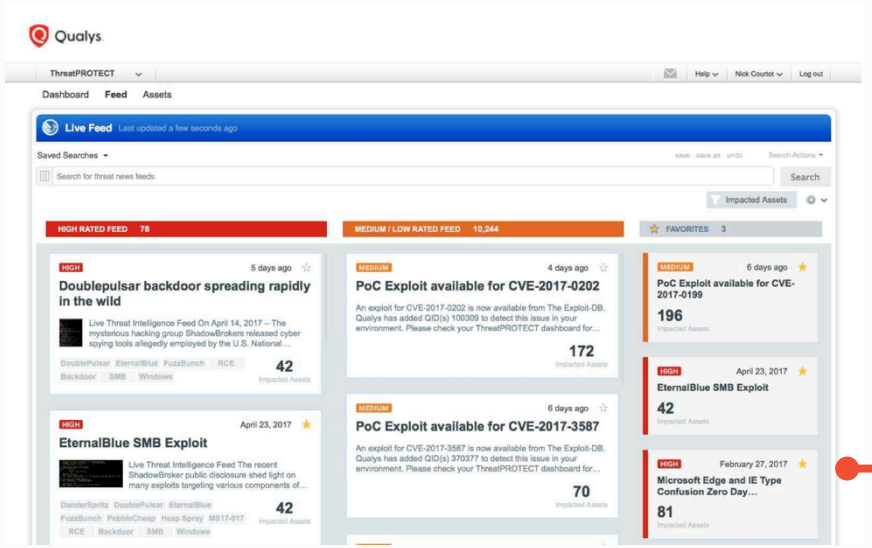
Intelligence Leveraged

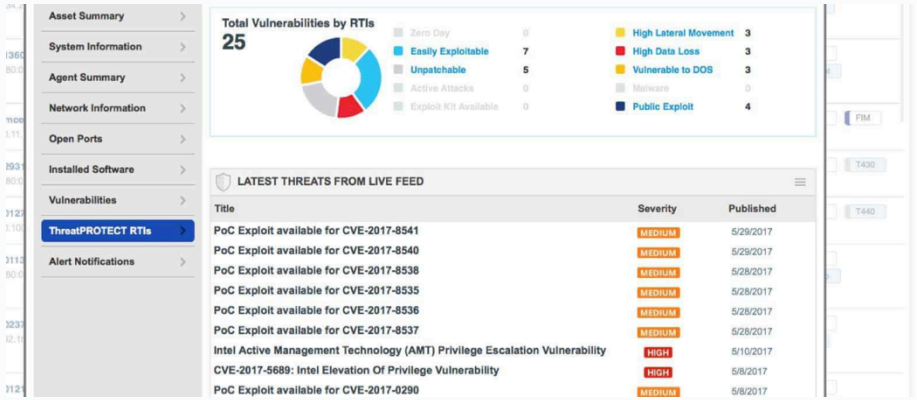


1. 21,409 vulnerabilities on 775 servers (2017).
2. Average Resolution 21.5 days.
3. Higher numbers than 2015.
4. Removal of Secondary Scanner Appliance (Nessus).
5. Priorities defined by risk.
6. Transitioned from reactive to proactive!

Qualys.

Actionable Vulnerability Information





Qualys Asset Inventory

Accurate server inventory with detailed and continuous hardware and software visibility.

Timely and actionable information to help prioritize decision making regarding EOL software and hardware.

Enable Efficiency Across IT and Security with Up to Date Continuous Visibility

Replaces manual procurement collection efforts.

Identify and know the assets on your network by functional category.

Prioritize replacing EOL hardware and software licensing with easy and efficient decision making.

Beta testing at Montana State University by Technical Leads in Distributed IT Units.

Could this improve the existing Server Inventory?

Tester Comment: *"I think it goes without saying this would be a huge improvement. The current Server Inventory is not easy to use and it's function is generally a mystery to end users."*

Thank You

Constantine Vorobetz
@qualys.com